#3

Atty. Dkt. No. 044499/0108

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Junichiro Yamada et al.

Title: PERSONAL IDENTIFICATION DEVICE AND METHOD

Appl. No.: 09/524,693

Filing Date: 3/14/2000

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japan Patent Application No. 11-073561 filed 3/18/1999.

Respectfully submitted,

JUN 6 2000

Date _____

By _____

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Attorney for Applicant
Registration No. 26,874

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　３月１８日

出 願 番 号
Application Number: 平成１１年特許願第０７３５６１号

出 願 人
Applicant (s): オムロン株式会社

２０００年　３月３１日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３０２１４７９

【書類名】　特許願

【整理番号】　OM58281

【提出日】　平成11年 3月18日

【あて先】　特許庁長官殿

【国際特許分類】　G06T 7/00

【発明者】

【住所又は居所】　京都府京都市右京区花園土堂町１０番地　オムロン株式会社内

【氏名】　山田　純一郎

【発明者】

【住所又は居所】　京都府京都市右京区花園土堂町１０番地　オムロン株式会社内

【氏名】　西川　義治

【特許出願人】

【識別番号】　000002945

【氏名又は名称】　オムロン株式会社

【代表者】　立石　義雄

【代理人】

【識別番号】　100069431

【弁理士】

【氏名又は名称】　和田　成則

【電話番号】　03(3295)1480

【手数料の表示】

【予納台帳番号】　014270

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9800578

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　個人認証方法および装置

【特許請求の範囲】

【請求項１】　ユーザの生体的特徴を検出し、該検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う個人認証方法において、

上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データをユーザが携帯する携帯記憶媒体に記憶し、

上記携帯記憶媒体から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行う

ことを特徴とする個人認証方法。

【請求項２】　上記携帯記憶媒体に、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、

上記ユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行う

ことを特徴とする請求項１記載の個人認証方法。

【請求項３】　上記携帯記憶媒体に、上記生体的特徴データを記憶し、

上記ユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行う

ことを特徴とする請求項１記載の個人認証方法。

【請求項４】　ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、

上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、

上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、

上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段と、

を具備することを特徴とする個人認証装置。

【請求項５】　上記携帯記憶媒体は、

上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行う

ことを特徴とする請求項４記載の個人認証装置。

【請求項６】　上記携帯記憶媒体は、

上記生体的特徴データを記憶し、

上記認証条件データ読取手段は、

上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行う

ことを特徴とする請求項４記載の個人認証装置。

【請求項７】　ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、

センタ装置と、

上記センタ装置に接続された複数の個人認証端末と、

を具備し、

上記個人認証端末は、

上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、

上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、

上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的

特徴データと照合することでユーザの個人認証を行う認証手段と、

上記センタ装置と通信を行う通信手段と、

を具備することを特徴とする個人認証装置。

【請求項８】　上記携帯記憶媒体は、

上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行う

ことを特徴とする請求項７記載の個人認証装置。

【請求項９】　上記携帯記憶媒体は、

上記生体的特徴データを記憶し、

上記認証条件データ読取手段は、

上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、

上記生体的特徴検出手段は、

上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行う

ことを特徴とする請求項７記載の個人認証装置。

【請求項１０】　上記センタ装置は、

各ユーザの上記生体的特徴データを記憶管理し、上記個人認証端末との間の通信により該記憶管理する各ユーザの上記生体的特徴データの更新処理を実行するとともに、上記個人認証端末によるユーザの認識結果を統括制御する

ことを特徴とする請求項７記載の個人認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ユーザの指紋、声紋、顔面等の生体的特徴を用いて個人認証を行う個人認証方法および装置に関し、詳しくは、ユーザが携帯するＩＣカード等の

携帯記憶媒体に記憶された認証条件データに基づき個人認証に使用する生体的特徴を特定して個人認証を行うようにした個人認証方法および装置に関する。

【０００２】

【従来の技術】

最近、カーナビゲーション、ノートパーソナルコンピュータ、電子手帳、各種モバイブル機器等においては指紋、声紋、顔面等の生体的特徴を用いて個人認証を行う個人認証装置が採用されている。

【０００３】

この指紋認証装置は、ユーザの特定の指の指紋データ、声紋データ、顔面の画像データ等の複数の生体的特徴を示すデータ（以下、これをバイオデータという）を予め登録しておき、装置の起動時等に際しては、この予め登録しておいたバイオデータと使用者から取得したバイオデータとを照合することで個人認証を行い、これにより他人による不正使用等を防止するようにしたものである。

【０００４】

【発明が解決しようとする課題】

しかし、上記従来の個人認証装置は、いずれもユーザの１つの生体的特徴に着目して構成されたもので、例えば、指紋を用いたものであれば指紋認証端末として構成され、声紋を用いたものであれば、声紋認証端末として構成され、顔面を用いたものであれば画像認証端末として構成されている。

【０００５】

ところが、ユーザの１つの特定の生体的特徴に着目して構成された個人認証装置においては、障害者や怪我人には使用できない場合もあり、また、正確な個人認証を行うことができない場合がある。

【０００６】

そこで、ユーザの複数の生体的特徴に着目して個人認証を行う構成も提案されているが、この場合は、指紋認証端末と声紋認証端末との組み合わせ、声紋認証端末と画像認証端末との組み合わせのように複数の認証端末を用いるものであり、いずれの場合も個人認証に用いることができる生体的特徴が固定されているので、自由度に乏しく、また、装置も大型化するという問題があった。

【０００７】

そこで、この発明は、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能であり、かつ高いセキュリティを実現できる個人認証方法および装置を提供することを目的とする。

【０００８】

【課題を解決するための手段】

上記目的を達成するため、請求項１記載の発明によれば、ユーザの生体的特徴を検出し、該検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う個人認証方法であって、上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データをユーザが携帯する携帯記憶媒体に記憶し、上記携帯記憶媒体から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行う。

【０００９】

このような構成によると、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になる。

【００１０】

また、請求項２記載の発明によれば、請求項１記載の発明において、上記携帯記憶媒体に、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うことを特徴とする。

【００１１】

このような構成によると、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる。

【００１２】

また、請求項３記載の発明によれば、請求項１記載の発明において、上記携帯記憶媒体に、上記生体的特徴データを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うことを特徴とする。

【００１３】

このような構成によると、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

【００１４】

また、請求項４記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、

１）上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段

２）上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段

３）上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段

を具備して構成される。

【００１５】

このような構成によると、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になる。

【００１６】

また、請求項５記載の発明によれば、請求項４記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うことを特徴とする。

【００１７】

このような構成によると、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる。

【００１８】

また、請求項６記載の発明によれば、請求項４記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、

上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うことを特徴とする。

【００１９】

このような構成によると、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

【００２０】

また、請求項７記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、センタ装置と、上記センタ装置に接続された複数の個人認証端末と、を具備し、上記個人認証端末は、上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段と、上記センタ装置と通信を行う通信手段と、を具備して構成される。

【００２１】

このような構成によると、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になるとともに、この個人認証を集中管理することが可能になる。

【００２２】

また、請求項８記載の発明によれば、請求項７記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うことを特徴とする。

【００２３】

このような構成によれば、請求項７の発明の効果に加えて、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になるという効果を奏する。

【００２４】

また、請求項９記載の発明によれば、請求項７記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うことを特徴とする。

【００２５】

このような構成によれば、請求項７の発明の効果に加えて、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

【００２６】

また、請求項１０記載の発明によれば、請求項７記載の発明において、上記センタ装置は、各ユーザの上記生体的特徴データを記憶管理し、上記個人認証端末との間の通信により該記憶管理する各ユーザの上記生体的特徴データの更新処理を実行するとともに、上記個人認証端末によるユーザの認識結果を統括制御することを特徴とする。

【００２７】

このような構成によれば、請求項７の発明の効果に加えて、個人認証に用いる生体的特徴データの集中管理も可能になる。

【００２８】

【発明の実施の形態】

以下、この発明に係わる個人認証方法および装置の実施の形態を添付図面を参照して詳細に説明する。

【００２９】

図１は、この発明に係わる個人認証装置の一実施の形態を示す斜視図である。

【００３０】

図１において、この個人認証装置１００は、ユーザの特定の指の指紋データ、声紋データ、顔面の画像データ等の複数の生体的特徴を示すデータ（バイオデータという）を用いて個人認証を行うもので、ユーザの特定の指の指紋データを採取するためのＣＣＤセンサ２０、ユーザの声紋データを採取するためのマイクロフォン３０、ユーザの顔面の画像データを採取するためのビデオカメラ４０が設けられている。

【００３１】

また、各種情報の表示機能および各種情報の入力を行う表示入力パネル部１０およびユーザが携帯可能な記憶媒体であるＩＣカード２００を挿入可能な挿入口５０が設けられている。

【００３２】

この実施の形態の個人認証装置１００は、個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データをユーザが携帯するＩＣカード２００に記憶し、このＩＣカード２００から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行うように構成される。

【００３３】

ここで、認証条件データとは、個人認証を行うために使用する生体的特徴（以下、バイオという）を特定するデータで、この実施の形態の個人認証装置１００においては、この認証条件データをＩＣカード２００から読み取り、この認証条件データに基づきユーザの個人認証を行うバイオを決定する。

【００３４】

具体的には、この実施の形態の個人認証装置１００においては、個人認証に使用可能なバイオとして

１）ユーザの特定の指の指紋

２）声紋

３）顔面の画像

４）サイン

の４種類が設定されており、認証条件データはこれら４種類のバイオのうちの１つまたは複数の選択を示すデータである。

【００３５】

図２は、図１に示した個人認証装置の詳細構成を示すブロック図である。

【００３６】

図２において、この個人認証装置１００は、表示入力パネル部１０、ＣＣＤセンサ２０、マイクロフォン３０、ビデオカメラ４０、周辺制御部６０、ＩＣカードライタリーダ（ＩＣカードＲ／Ｗ）７０、メモリ８０、中央演算処理部（ＣＰＵ）９０を具備して構成される。また、周辺制御部６０は、有線または無線の回線３０１を介してセンタ装置３００に通信可能に接続されている。

【００３７】

ここで、表示入力パネル部１０は、液晶表示装置（ＬＣＤ）１０－１およびタッチパネル１０－２を具備して構成され、液晶表示装置（ＬＣＤ）１０－１上にタッチパネル１０－２を載置した構成をとることにより、各種情報の表示機能および各種情報の入力機能を実現している。

【００３８】

ＣＣＤカメラ２０は、周辺制御部６０に接続され、この周辺制御部６０の制御のもとにこの個人認証装置１００の使用可能なバイオの１つであるユーザの特定の指の指紋に基づき指紋データを読み取るものである。

【００３９】

また、マイクロフォン３０は、周辺制御部６０に接続され、この周辺制御部６０の制御のもとにこの個人認証装置１００の使用可能なバイオの他の１つであるユーザの声紋に対応する声紋データを取り込むものである。

【００４０】

また、ビデオカメラ４０は、周辺制御部６０に接続され、この周辺制御部６０の制御のもとにこの個人認証装置１００の使用可能なバイオの更に他の１つであるユーザの顔面に対応する画像データを取り込むものである。

【００４１】

周辺制御部６０は、ＣＣＤカメラ２０およびマイクロフォン３０およびビデオ

カメラ４０に接続されるとともにＩＣカードＲ／Ｗ７０およびＣＰＵ９０および表示入力パネル部１０に接続され、ＣＣＤカメラ２０およびマイクロフォン３０およびビデオカメラ４０による指紋データおよび声紋データおよび顔面の画像データの取り込みを制御するとともに、ＩＣカードＲ／Ｗ７０によるＩＣカード２００からのデータの読み出し書き込み動作および表示入力パネル部１０による情報表示入力動作を制御する。

【００４２】

また、周辺制御部６０は、回線３０１を介してセンタ装置３００に接続されており、センタ装置３００との通信に基づき各種データの送受を行う。

【００４３】

ここで、センタ装置３００は、各ユーザのバイオデータを記憶管理し、個人認証装置１００との間の通信によりこの記憶管理する各ユーザのバイオデータの更新処理を実行するとともに、個人認証装置１００によるユーザの認識結果を統括制御する。

【００４４】

メモリ８０は、ＣＰＵ９０を動作させるための制御プログラムとともにこの個人認証装置１００の制御に必要な各種情報を記憶している。

【００４５】

ＯＰＵ９０は、周辺制御部６０に接続されるとともに、メモリ８０に接続されており、メモリ８０に記憶された情報に基づき、周辺制御部６０を介して、この個人認証装置１００の各部の動作を統括制御する。

【００４６】

図３は、図１および図２に示したＩＣカードに記憶されている情報の一例を示す図である。

【００４７】

図３に示す構成において、図１および図２に示したＩＣカード２００には、バイオ実行条件テーブル２０１、指紋バイオ実装テーブル２０２、声紋バイオ実装テーブル２０３、顔面バイオ実装テーブル２０４、指紋本人データ２０５、声紋本人データ２０６、顔面本人データ２０７等が格納されている。

【００４８】

ここで、バイオ実行条件テーブル２０１は、上述した認証条件データを記憶するテーブルである。

【００４９】

また、指紋バイオ実装テーブル２０２および声紋バイオ実装テーブル２０３および顔面バイオ実装テーブル２０４は、それぞれ指紋本人データ２０５および声紋本人データ２０６および顔面本人データ２０７の実装、非実装を示すデータが格納される。

【００５０】

ここで、このデータは、「１」または「０」の２値からなり、「１」は対応するバイオデータの実装を示し、「０」は対応するバイオデータの非実装を示す。

【００５１】

また、指紋本人データ２０５は、ユーザ本人から予め取得して登録したユーザの特定の指の指紋に対応する指紋データであり、声紋本人データ２０６は、ユーザ本人から予め取得して登録したユーザの声紋に対応する声紋データであり、顔面本人データ２０７は、ユーザ本人から予め取得して登録したユーザの画面に対応する画像データである。

【００５２】

図４は、図１および図２に示したＩＣカードに記憶されている情報の他の例を示す図である。

【００５３】

図４においては、図３に示した構成に加えて、指紋認証アルゴリズム２０５－１、声紋認証アルゴリズム２０６－１、顔面認証アルゴリズム２０７－１が格納されている。

【００５４】

すなわち、図４に示す構成においては、図１および図２に示したＩＣカード２００には、バイオ実行条件テーブル２０１、指紋バイオ実装テーブル２０２－１、声紋バイオ実装テーブル２０３－１、顔面バイオ実装テーブル２０４－１、指紋認証アルゴリズム２０５－１、指紋本人データ２０５、声紋認証アルゴリズム

２０６－１、声紋本人データ２０６、顔面認証アルゴリズム２０７－１、顔面本人データ２０７等が格納されている。

【００５５】

ここで、バイオ実行条件テーブル２０１は、上述した認証条件データを記憶するテーブルである。

【００５６】

また、指紋バイオ実装テーブル２０２－１および声紋バイオ実装テーブル２０３－１および顔面バイオ実装テーブル２０４－１は、それぞれ指紋本人データ２０５および声紋本人データ２０６および顔面本人データ２０７の実装、非実装および認証処理をＩＣカード２００内部で行うか否かを示すデータが格納される。

【００５７】

ここで、このデータは、「１」、「０」、「－１」の３値からなり、「１」は対応するバイオデータの実装を示し、「０」は対応するバイオデータの非実装を示す。また、「－１」は、対応するバイオを用いた認証処理をＩＣカード２００内部で行うことを示す。

【００５８】

また、指紋認証アルゴリズム２０５－１、声紋認証アルゴリズム２０６－１、顔面認証アルゴリズム２０７－１は、指紋データ、声紋データ、顔面に対応する画像データをを用いた指紋認証アルゴリズム、声紋認証アルゴリズム、顔面認証アルゴリズムを示す。

【００５９】

また、指紋本人データ２０５は、ユーザ本人から予め取得して登録したユーザの特定の指の指紋に対応する指紋データであり、声紋本人データ２０６は、ユーザ本人から予め取得して登録したユーザの声紋に対応する声紋データであり、顔面本人データ２０７は、ユーザ本人から予め取得して登録したユーザの画面に対応する画像データである。

【００６０】

すなわち、図４に示した構成においては、ＩＣカード２００内部に指紋認証、声紋認証、顔面認証を行うアルゴリズムをそれぞれ内蔵しており、これにより、

ＩＣカード２００内部において、指紋認証、声紋認証、顔面認証を行うことができるように構成されている。

【００６１】

図５は、図１および図２に示した個人認証装置における個人認証動作を示すフローチャートである。

【００６２】

なお、図５に示すフローチャートは、ＩＣカード２００内に記憶されるデータが図４に示す構成をとる場合の個人認証装置１００の処理を示している。

【００６３】

図５において、この処理が開始されると、まず、この個人認証装置１００の挿入口５０にユーザの形態するＩＣカード２００が挿入されたかを調べる（ステップ１０１）。ここで、ＩＣカード２００が挿入されていないと判断されると（ステップ１０１でＮＯ）、ステップ１０１に戻り、この個人認証装置１００の挿入口５０にユーザの形態するＩＣカード２００が挿入されるのを待つ。

【００６４】

ステップ１０１で、この個人認証装置１００の挿入口５０にユーザの形態するＩＣカード２００が挿入されたと判断されると（ステップ１０１でＹＥＳ）、ＩＣカードＲ／Ｗ７０によりＩＣカード２００内のデータの読み込みが行われる（ステップ１０２）。

【００６５】

そして、ＩＣカード２００内から読み取ったデータのうちのバイオ実行条件テーブル２０１の内容に基づき表示入力パネル部１０を用いて個人認証に使用するバイオの案内表示を行う（ステップ１０３）。

【００６６】

次に、ユーザの特定の指の指紋データを採取するためのＣＣＤセンサ２０、ユーザの声紋データを採取するためのマイクロフォン３０、ユーザの顔面の画像データを採取するためのビデオカメラ４０を駆動してユーザからバイオ認証データを取得する（ステップ１０４）。

【００６７】

そして、ＩＣカード２００内から読み取ったデータのうちの指紋バイオ実装テーブル２０２－１および声紋バイオ実装テーブル２０３－１および顔面バイオ実装テーブル２０４－１を参照して、バイオ実装テーブルは内部指定か、すなわち、バイオの認証をＩＣカード２００内で行うか否かの判定を行う（ステップ１０５）。

【００６８】

例えば、指紋バイオ実装テーブル２０２－１の内容が、「１」の場合は、指紋バイオデータの実装を示し、「０」の場合は、指紋バイオデータの非実装を示し、「－１」の場合は、指紋バイオを用いた認証処理をＩＣカード２００内部で行うことを示す。

【００６９】

同様に、声紋バイオ実装テーブル２０３－１の内容が、「１」の場合は、声紋バイオデータの実装を示し、「０」の場合は、声紋バイオデータの非実装を示し、「－１」の場合は、声紋バイオを用いた認証処理をＩＣカード２００内部で行うことを示し、顔面バイオ実装テーブル２０４－１の内容が、「１」の場合は、顔面バイオデータの実装を示し、「０」の場合は、顔面バイオデータの非実装を示し、「－１」の場合は、顔面バイオを用いた認証処理をＩＣカード２００内部で行うことを示す。

【００７０】

ここで、バイオ実装テーブルは内部指定でない、すなわち、バイオの認証をＩＣカード２００内では行わないと判断された場合は（ステップ１０５でＮＯ）、端末側、すなわち個人認証装置１００側の認証アルゴリズムを駆動して認証動作を行う（ステップ１０６）。

【００７１】

また、ステップ１０５で、バイオ実装テーブルは内部指定である、すなわち、バイオの認証をＩＣカード２００内で行うと判断された場合は（ステップ１０５でＹＥＳ）、ＩＣカード２００へユーザから取得したバイオ認証データを転送し（ステップ１０９）、ＩＣカード２００側の認証アルゴリズムを駆動して認証動作を行い（ステップ１１０）、その認証結果を端末、すなわち、個人認証装置１

００に通知する（ステップ１１１）。

【００７２】

次に、バイオ実装テーブルで複数の指定終了か、すなわち、指定した全てのバイオを用いた認証動作が終了かを調べる（ステップ１０７）。ここで、バイオ実装テーブルで複数の指定終了でない、すなわち、指定した全てのバイオを用いた認証動作が終了していないと判断された場合は（ステップ１０７でＮＯ）、ステップ１０３に戻り、ステップ１０３からステップ１０７の処理を繰り返す。

【００７３】

そして、ステップ１０７で、バイオ実装テーブルで複数の指定終了、すなわち、指定した全てのバイオを用いた認証動作が終了したと判断されると（ステップ１０７でＹＥＳ）、その認証結果を出力して表示入力パネル部１０に表示し（ステップ１０８）、この処理を終了する。

【００７４】

なお、上記説明においてはＩＣカード２００内に記憶されるデータが図４に示す構成をとる場合の個人認証装置１００の処理を示したが、ＩＣカード２００内に記憶されるデータが図３に示す構成をとる場合は、全ての認証処理が個人認証装置１００側で行われることになり、図５に示した処理のうちのステップ１０５の処理およびステップ１０９から１１１の処理が省略される。

【００７５】

【発明の効果】

以上説明したように、請求項１記載の発明によれば、ユーザの生体的特徴を検出し、該検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う個人認証方法であって、上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データをユーザが携帯する携帯記憶媒体に記憶し、上記携帯記憶媒体から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行うように構成したので、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になるとともに高いセキュリティが実現できる。

【００７６】

また、請求項２記載の発明によれば、請求項１記載の発明において、上記携帯記憶媒体に、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うように構成したので、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる。

【００７７】

また、請求項３記載の発明によれば、請求項１記載の発明において、上記携帯記憶媒体に、上記生体的特徴データを記憶し、上記ユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うように構成したので、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる。

【００７８】

また、請求項４記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段とを具備して構成したので、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になるとともに高いセキュリティが実現できる個人認証装置を提供することができる。

【００７９】

また、請求項５記載の発明によれば、請求項４記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個

人認証を行うように構成したので、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる個人認証装置を提供することができる。

【００８０】

また、請求項６記載の発明によれば、請求項４記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うように構成したので、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる個人認証装置を提供することができる。

【００８１】

また、請求項７記載の発明によれば、ユーザの生体的特徴を用いて個人認証を行う個人認証装置において、センタ装置と、上記センタ装置に接続された複数の個人認証端末と、を具備し、上記個人認証端末は、上記個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データを記憶したユーザが携帯する携帯記憶媒体から上記認証条件データを読み取る認証条件データ読取手段と、上記認証条件データ読取手段により読み取った認証条件データに対応する生体的特徴をユーザから検出する生体的特徴検出手段と、上記生体的特徴検出手段で検出した生体的特徴を予め取得したユーザの生体的特徴データと照合することでユーザの個人認証を行う認証手段と、上記センタ装置と通信を行う通信手段と、を具備して構成したので、ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能になるとともに、この個人認証を集中管理することが可能になる個人認証装置を提供することができる。

【００８２】

また、請求項８記載の発明によれば、請求項７記載の発明において、上記携帯記憶媒体は、上記生体的特徴データとともに上記生体的特徴を用いた個人認証の

認証アルゴリズムを記憶し、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体に転送することで個人認証を行うように構成したので、請求項７の発明の効果に加えて、ある生体的特徴データに関して装置本体内に認証アルゴリズムを持たない場合にも個人認証が可能になる個人認証装置を提供することができる。

【００８３】

また、請求項９記載の発明によれば、請求項７記載の発明において、上記携帯記憶媒体は、上記生体的特徴データを記憶し、上記認証条件データ読取手段は、上記認証条件データとともに上記生体的特徴データを上記携帯記憶媒体から読み取り、上記生体的特徴検出手段は、上記生体的特徴検出手段によりユーザから検出した生体的特徴を上記携帯記憶媒体から読み取った上記生体的特徴データと照合することで個人認証を行うように構成したので、請求項７の発明の効果に加えて、装置本体内には参照対象となる生体的特徴データを記憶しなくてよくなるので複数の生体的特徴データを用いた個人認証を大きな自由度をもって実現することが可能になる個人認証装置を提供することができる。

【００８４】

また、請求項１０記載の発明によれば、請求項７記載の発明において、上記センタ装置は、各ユーザの上記生体的特徴データを記憶管理し、上記個人認証端末との間の通信により該記憶管理する各ユーザの上記生体的特徴データの更新処理を実行するとともに、上記個人認証端末によるユーザの認識結果を統括制御するように構成したので、請求項７の発明の効果に加えて、個人認証に用いる生体的特徴データのを集中管理が可能になる個人認証装置を提供することができるという効果を奏する。

【図面の簡単な説明】

【図１】

この発明に係わる個人認証装置の一実施の形態を示す斜視図である。

【図２】

図１に示した個人認証装置の詳細構成を示すブロック図である。

【図３】

図１および図２に示したＩＣカードに記憶されている情報の一例を示す図である。

【図４】

図１および図２に示したＩＣカードに記憶されている情報の他の例を示す図である。

【図５】

図１および図２に示した個人認証装置における個人認証動作を示すフローチャートである。

【符号の説明】

１０　表示入力パネル部

２０　ＣＣＤセンサ

３０　マイクロフォン

４０　ビデオカメラ

５０　ＩＣカード挿入口

６０　周辺制御部

７０　ＩＣカードライタリーダ（ＩＣカードＲ／Ｗ）

８０　メモリ

９０　中央演算処理部（ＣＰＵ）

１００　個人認証装置

２００　ＩＣカード

２０１　バイオ実行条件テーブル

２０２　指紋バイオ実装テーブル

２０２－１　指紋バイオ実装テーブル

２０３　声紋バイオ実装テーブル

２０３－１　声紋バイオ実装テーブル

２０４　顔面バイオ実装テーブル

２０４－１　顔面バイオ実装テーブル

２０５　指紋本人データ

２０５－１　指紋認証アルゴリズム

２０６　　声紋本人データ

２０６－１　　声紋認証アルゴリズム

２０７　　顔面本人データ

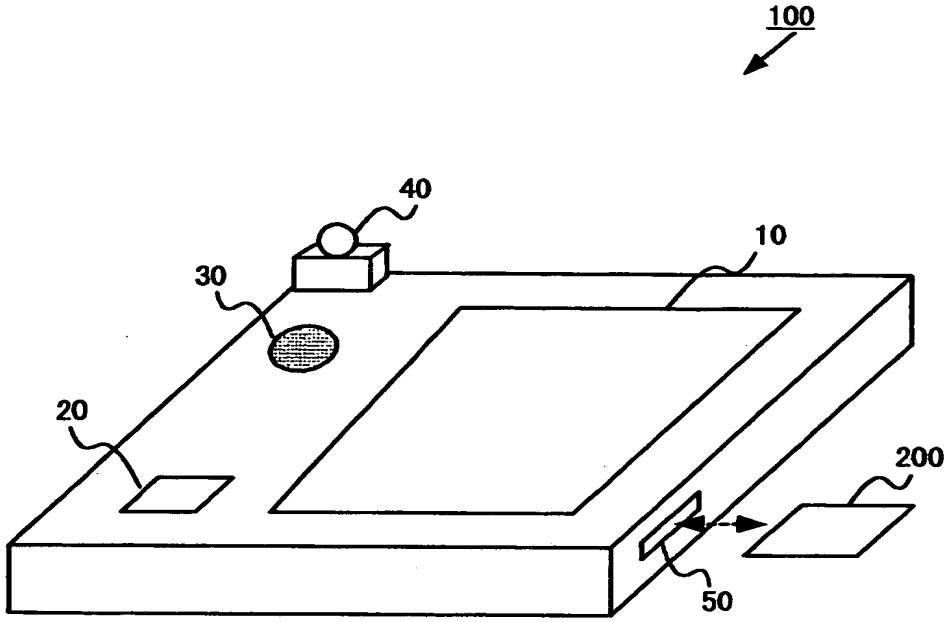
２０７－１　　顔面認証アルゴリズム

３００　　センタ装置

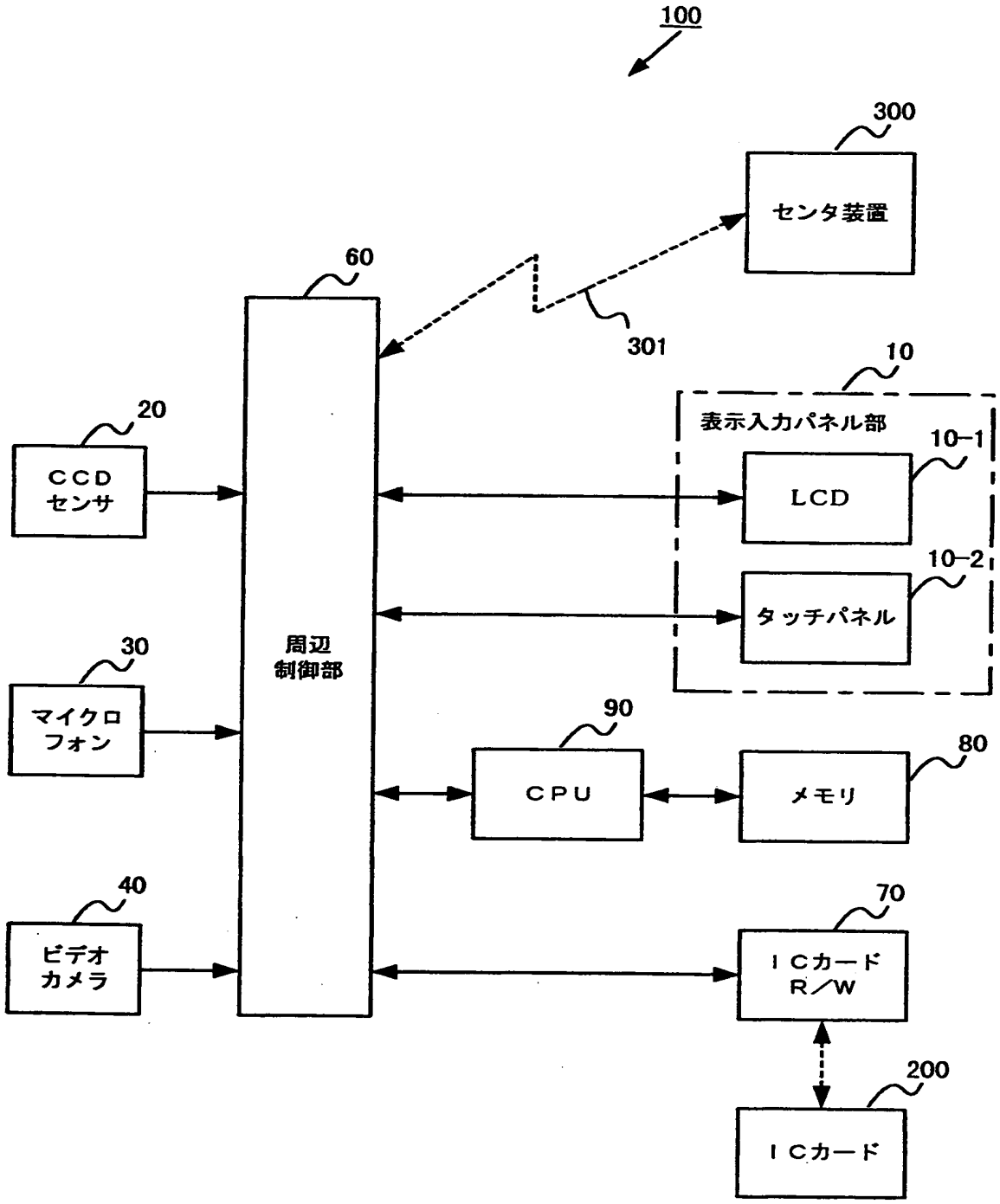
３０１　　回線

【書類名】　図面

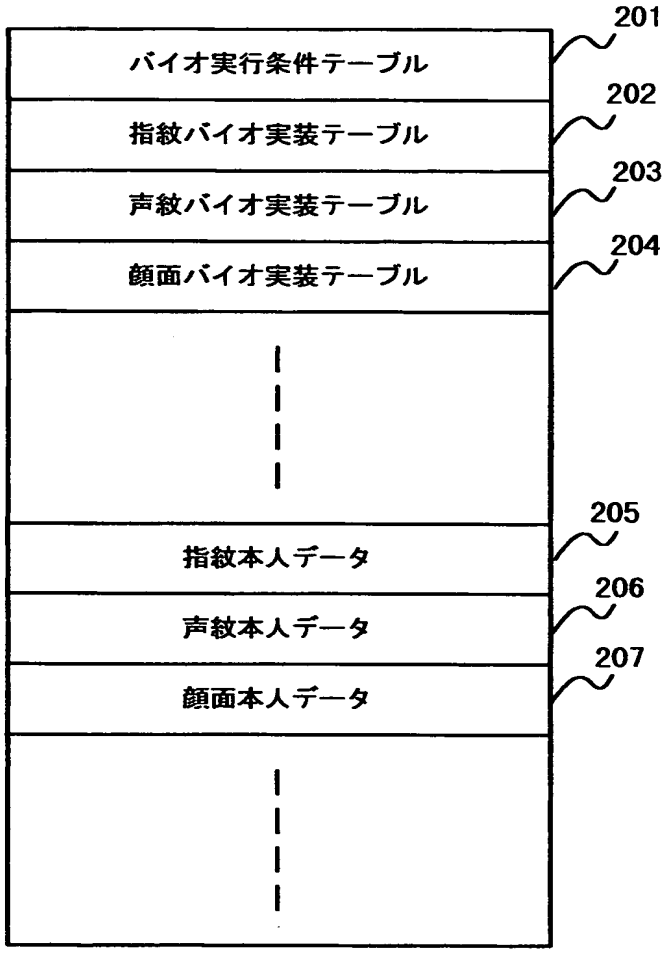
【図１】



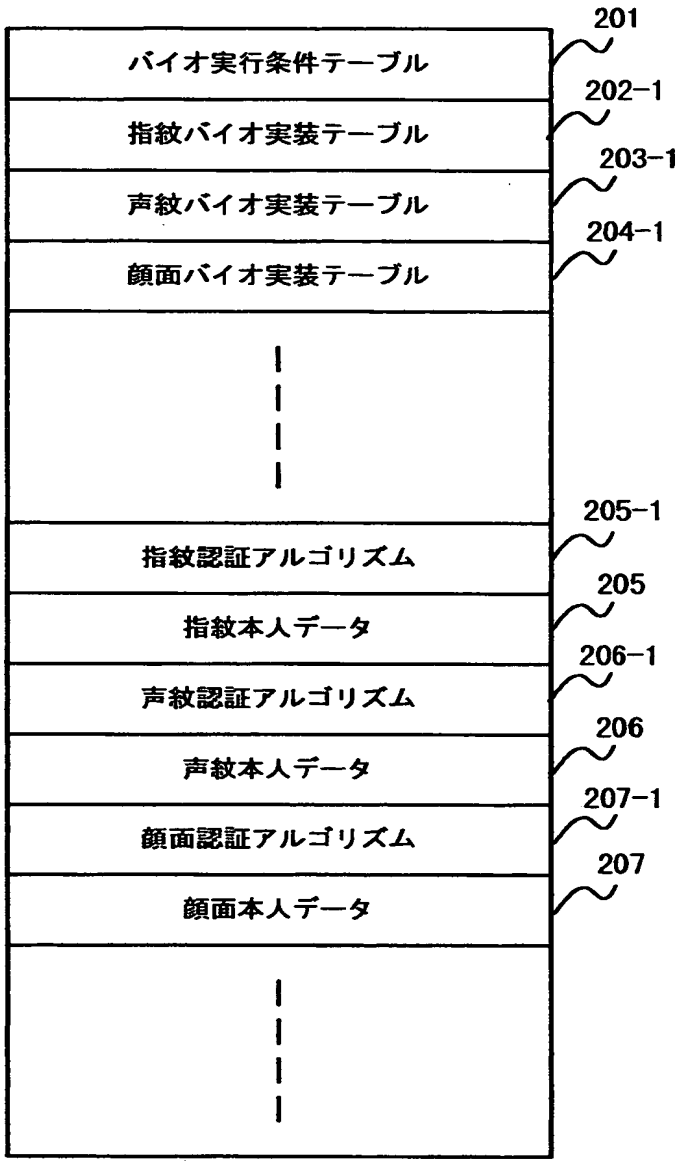
【図２】


100
300
センタ装置
60
301
10
表示入力パネル部
20
CCD
センサ
10-1
LCD
10-2
タッチパネル
30
マイクロ
フォン
周辺
制御部
90
CPU
80
メモリ
40
ビデオ
カメラ
70
ＩＣカード
R／W
200
ＩＣカード

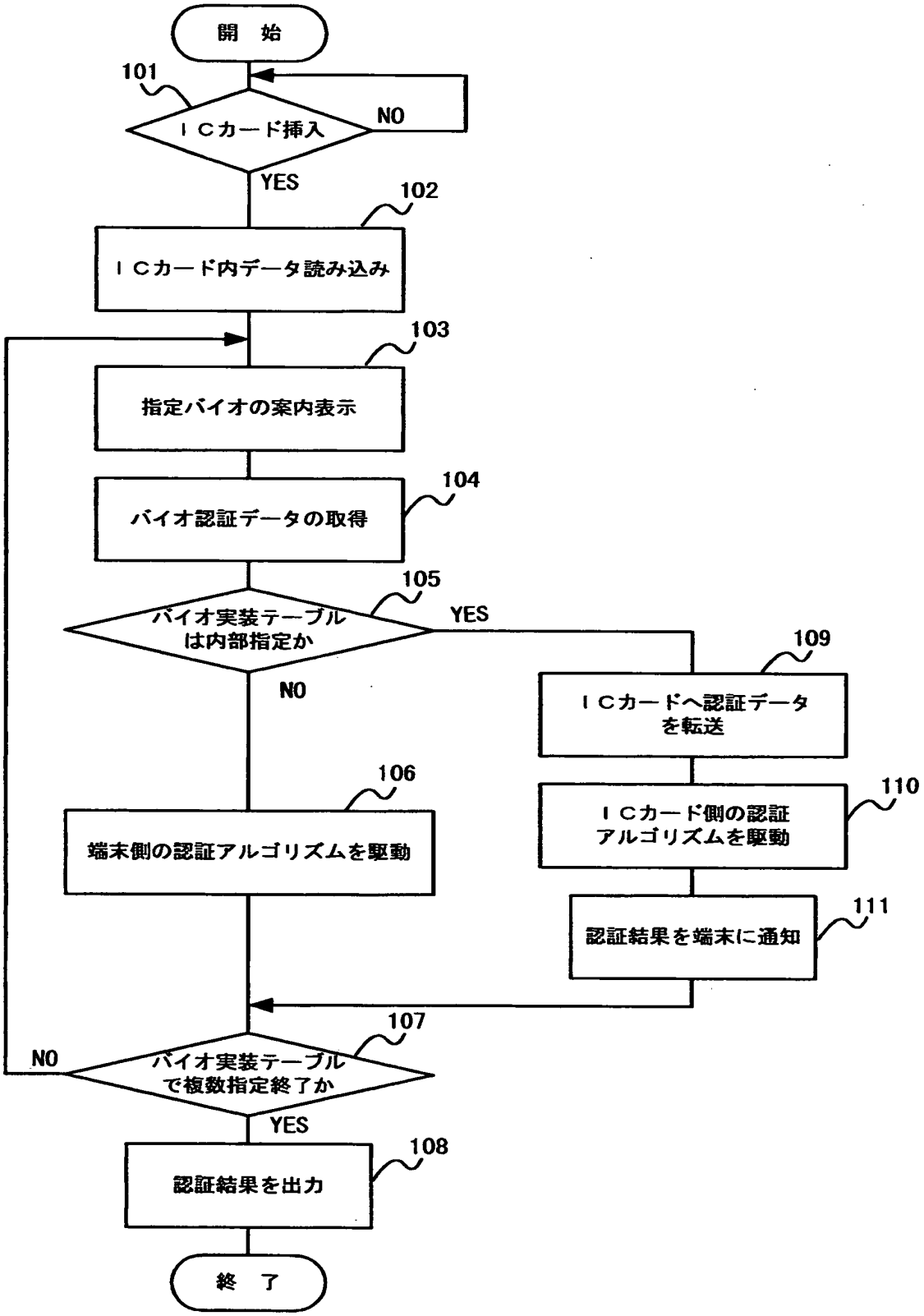
【図３】


201
バイオ実行条件テーブル
202
指紋バイオ実装テーブル
203
声紋バイオ実装テーブル
204
顔面バイオ実装テーブル
205
指紋本人データ
206
声紋本人データ
207
顔面本人データ

【図４】


201
バイオ実行条件テーブル
202-1
指紋バイオ実装テーブル
203-1
声紋バイオ実装テーブル
204-1
顔面バイオ実装テーブル
205-1
指紋認証アルゴリズム
205
指紋本人データ
206-1
声紋認証アルゴリズム
206
声紋本人データ
207-1
顔面認証アルゴリズム
207
顔面本人データ

【図５】


開　始
101
ＩＣカード挿入
NO
YES
102
ＩＣカード内データ読み込み
103
指定バイオの案内表示
104
バイオ認証データの取得
105
バイオ実装テーブル
は内部指定か
YES
NO
109
ＩＣカードへ認証データ
を転送
106
端末側の認証アルゴリズムを駆動
110
ＩＣカード側の認証
アルゴリズムを駆動
111
認証結果を端末に通知
107
NO
バイオ実装テーブル
で複数指定終了か
YES
108
認証結果を出力
終　了

【書類名】　要約書

【要約】

【課題】　ユーザの要望に合わせた複数の生体的特徴を用いる個人認識が可能であり、かつ高いセキュリティを実現できる個人認証方法および装置を提供する。

【解決手段】　個人認証を行うための少なくとも１つの生体的特徴を特定する認証条件データをユーザが携帯するＩＣカード２００に記憶し、このＩＣカード２００から読み取った認証条件データに対応する生体的特徴をユーザから検出することで個人認証を行う。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２９４５〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　京都府京都市右京区花園土堂町１０番地
氏　名　オムロン株式会社